NAVAL WAR COLLEGE
Newport, R.I.

# CRITICAL FACTORS IN CYBERSPACE

by
John Van Cleave
Lieutenant Commander, U.S. Navy

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: J A Van Cle

08 November 1997

Paper directed by
G. W. Jackson, Captain, U.S. Navy
Chairman, Department of Joint Military Operations

Mark Welch 6FEB97
Faculty Advisor Date
Mark Welch, Commander, U.S. Navy

UNCLASSIFIED
Security Classification This Page

# REPORT DOCUMENTATION PAGE

1. **Report Security Classification:** UNCLASSIFIED

2. **Security Classification Authority:**

3. **Declassification/Downgrading Schedule:**

4. **Distribution/Availability of Report:** DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.

5. **Name of Performing Organization:** JOINT MILITARY OPERATIONS DEPARTMENT

6. **Office Symbol:** C

7. **Address:** NAVAL WAR COLLEGE
686 CUSHING ROAD
NEWPORT, RI 02841-1207

8. **Title** (Include Security Classification):

CRITICAL FACTORS IN CYBERSPACE (U)

9. **Personal Authors:**
JOHN A. VAN CLEAVE , LCDR, USN

10. **Type of Report:** FINAL

11. **Date of Report:** 7 FEBRUARY 1997

12. **Page Count:** 22

13. **Supplementary Notation:** A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. **Ten key words that relate to your paper:** CRITICAL FACTORS, CYBERSPACE, CRITICAL STRENGTHS, CRITICAL WEAKNESSES, CRITICAL VULNERABILITIES,

15. **Abstract:** Since WWII, warfare and conflict involving the United States, has taken on an "antiseptic" dimension. Conflicts have been resolved in far away places, separated by distance and a powerful military force able to project power and take the fight to the enemy. In doing so the U.S. has remained relatively immune to attacks on its own social, economic, political, and military infrastructures. But as the U.S. forges ahead into the information age, the global connectivity inherent in this transformation also brings about new vulnerabilities.

The vast advantages of space - the fabled "high ground" - including the civil and military capabilities it brings to the U.S will soon be overshadowed by what could be termed the "common ground", Cyberspace. In Cyberspace highly computerized and networked social, economic, political, and military infrastructures become intertwined, increasing their vulnerability to attack. This paper will explore some current and future challenges that must be considered carefully as we develop the new common ground in Cyberspace and the impact that cyber weapons will have in reshaping operational and strategic planning. It will also identify critical factors traditional in U.S. infrastructures that are increasingly vulnerable to attack through Cyberspace due to these new linkages.

Through the utility of Cyberspace, once secure lines of communication will lose the sanctuary created by strategic geography and a strong military force. It is now incumbent upon civil and military planners to recognize these emerging vulnerabilities and establish new "forces" and "objectives" which protect American interests in this new frontier. As they are presently configured, traditional military force may not be able to handle the new security challenges posed by Cyberspace.

| 16. Distribution / Availability of Abstract: | Unclassified | Same As Rpt | DTIC Users |
|---|---|---|---|
| | X | | |

17. **Abstract Security Classification:** UNCLASSIFIED

18. **Name of Responsible Individual:** CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT

19. **Telephone:** 841-6461

20. **Office Symbol:** C

Security Classification of This Page Unclassified

## Abstract of
## Critical Factors in Cyberspace

Since WWII, warfare and conflict involving the United States, has taken on an "antiseptic" dimension. Conflicts have been resolved in far away places, separated by distance and a powerful military force able to project power and take the fight to the enemy. In doing so the U.S. has remained relatively immune to attacks on its own social, economic, political, and military infrastructures. But as the U.S. forges ahead into the information age, the global connectivity inherent in this transformation also brings about new vulnerabilities.

The vast advantages of space - the fabled "high ground" - including the civil and military capabilities it brings to the U.S. will soon be overshadowed by what could be termed the "common ground", Cyberspace. In Cyberspace highly computerized and networked social, economic, political, and military infrastructures become intertwined, increasing their vulnerability to attack. This paper will explore some current and future challenges that must be considered carefully as we develop the new common ground in Cyberspace and the impact that cyber weapons will have in reshaping operational and strategic planning. It will also identify critical factors traditional in U.S. infrastructures that are increasingly vulnerable to attack through Cyberspace due to these new linkages.

Through the utility of Cyberspace, once secure lines of communication will lose the sanctuary created by strategic geography and a strong military force. It is now incumbent upon civil and military planners to recognize these emerging vulnerabilities and establish new “forces” and “objectives” which protect American interests in this new frontier. As they are presently configured, traditional military force may not be able to handle the new security challenges posed by Cyberspace.

## Introduction

With the possibility of resolving future conflicts by fighting in other than a "terrain-defined battlespace," some of the basic definitions of operational art will no doubt have to be expanded upon .[1] But first; what is Cyberspace? Some would say, "The sensation of place without location, or space without physicality, experienced while using global computer networks." [2] Joint Pub 1-02, the *DOD Dictionary of Military and Associated Terms*, makes no mention of Cyberspace. Definitions in various periodicals identify the Internet and the World Wide Web as vehicles which allow access into Cyberspace. Volume I of the *Joint Command and Control, Communications, and Computers Systems Descriptions* publication alludes to Cyberspace as it provides a synopsis on the capability of the up and coming Global Command and Control System (GCCS) which will provide the ability to "...pull information through a global, integrated infosphere." [3] What is important is the fact that through the utility of Cyberspace, computer systems will be "tied together" (networked) locally or globally. With the extensive integration of social, economic, political, and military information systems by such a vast network of computers and information sharing systems, the U.S. will no doubt benefit from the intrinsic advantages that shared information can provide. But these advantages are not without a cost. By their very nature of operation; these information systems have more global exposure than ever before, making them vulnerable to enemy deception, manipulation, and attack. [4]

Understanding the impact that Cyberspace has in exposing previously secure critical strengths, weaknesses, and vulnerabilities (critical factors) requires in part, a general overview of past conflicts and how they were fought. The United States' infrastructure has enjoyed the strategic luxury of being physically distanced from the enemy by vast expanses of ocean.

Coupled with a military force able to project power, the U.S. was fairly insulated from direct attacks on its home soil. The geography of the situation alone would probably be a deterrent considering the extensive lines of communication (LOC's) and logistic's sustainment required by an adversary in carrying out an attack. With the utility of Cyberspace, hurdles such as LOC's and complex logistics requirements for force sustainment can be bypassed. Figure (1) depicts the traditional U.S. security paradigm in which the military comes between the adversary and society. Through Cyberspace, sanctuary is lost as is illustrated in Figure (2).[5]

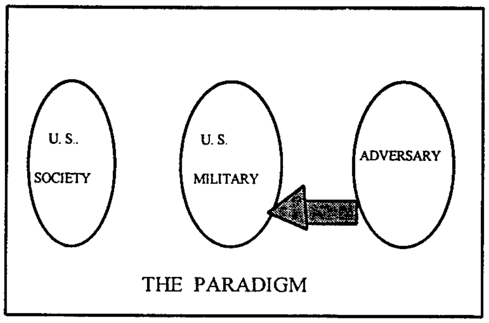

Figure 1. The Traditional Paradigm

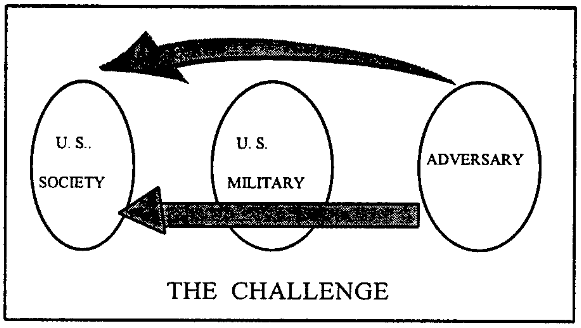

Figure 2. The Lost Sanctuary

The important consequence which the paradigm shift reveals is the opportunity Cyberspace provides to adversaries; a new dimension and approach for indirect or direct attacks on critical strengths, weaknesses, and vulnerabilities in our society. They are the new perimeter which must be defended if the enemy is to be defeated in his attempts to defeat our strategic center of gravity (COG). Our COG, which in the past may have required massive physical efforts to attack is now made vulnerable by the global connectivity of Cyberspace afforded by such systems as the "information superhighway."[6] It is therefore through Cyberspace, that a knowledgeable adversary may circumvent military force, and geography and exploit the once secure critical factors.[7]

## Vulnerability Characteristics within the Lost Sanctuary

Attacks on critical factors via Cyberspace will provide unique and challenging situations. Attacks could be very economical for a knowledgeable adversary to make since a minimal investment in hardware is all that is required; "for the price of a $2,000 computer and a $200 modem you potentially can throw a multibillion dollar, high-tech military such as the United States' into chaos."[8] As an example, if the transportation and logistics information systems were targeted, the timely and complex movement of men and material could be hampered by computer induced "glitches." Material could be lost and manpower delayed. In today's conflicts, timely response could be the key difference between deterrence and escalation. Contrasting this with the massive effort demonstrated in the Pacific during WWII in cutting off Japan's LOC's reveals that a modern day adversary would not require a large Navy to interdict U.S. LOC's if it can disrupt the supplying sources for those LOC's. Such a capability demonstrates the leverage that information technology provides and certainly bolsters the idea of an adversary's economy of force.

Attacks will also be capable of being generated by anyone with little or no warning making it difficult in assessing strategic or even tactical situations for decision makers even as reaction time shrinks.[9] Operational surprise may be even easier to achieve. Information will be susceptible to tainting or compromise without the knowledge of the end user manifesting a new dimension in operational deception.[10] Because of the interconnectivity in Cyberspace, traditional boundaries and jurisdictions may become fogged. Such obscurity could lead to confusion as to who is under attack or who should respond.[11] Systems which interconnect or utilize products generated via Cyberspace such as C4I and high tech weapons, the new bastions of the U.S., are vulnerable. Since the vast information-sharing network leaves few clues as to where an attack originated from or who conducted an attack, knowledge of how present and future Cyberspace weapons operate as well as their methods of employment are the only means by which defenses can be made.

## The Arsenal in Cyberspace

The array of weapons available for use in Cyberspace are numerous and complex. Some of the cyber weapons available are computer viruses; a subset of what is known in the computer world as "malicious codes."[12] Malicious codes come in different types and serve different functions which makes it important in understanding these codes. Viruses are characterized by being extremely efficient pieces of codes, often consisting of fewer than 100 bytes compiled. This simplicity of character and attack strategy is one of the reasons why computer viruses succeed. [13] They can be easily masked by the complexity of other computer programs, to which they become attached.

Worms are another subset of malicious codes and differ from viruses in one subtle but important way; a worm does not require a host [does not attach itself to a program]. "Whil virus can only be replicated by running an infected programme, a worm can take advantage of loopholes in an operating system applying a direct attack strategy."[14] As a worm self replicates, it can deny access to a system by overwhelming that system with its progeny.[15]

Trojan horses comprise a sinister subset of malicious codes since they are "designed to impersonate legitimate programmes."[16] Codes of this nature can allow for the theft of passwords in computer systems or the generation of surreptitious copies of data.

Logic bombs are usually improperly written legitimate code which were the result of faulty programming; the year 2000 problem for example. However, deliberate logic bombs such as a "trap door" may be used by unintended parties to bypass or shortcut security procedures."[17] Other types can be highly destructive and can lay dormant waiting for certain events to occur before destroying computer information.

A logic torpedo is a controlled virus which is aimed at one or more systems. Launched into Cyberspace, the logic torpedo tracks down its target (particular type of program) which it then infects.[18]

Time bombs are similar to logic bombs but are activated by a "specific time rather than a logic state."[19] A time weapon targets the internal clock of the computer which ultimately affects timing and synchronization leading to great difficulty in the system's ability to communicate.

Hybrid malicious codes produced by the "fusion" of viruses, worms, logic bombs, and trojan horses could be designed to "remain transparently dormant until a pre-determined time or series of events cue it to life. Once active, the virus may remain actively persistent or target a specific computer function before returning to its dormant state."[20]

Cyber weapons introduce challenging problems to the users of any computerized system. Most important of which are integrated computer network systems such as telecommunications, $C^2$, power grids, and air traffic control.[21] Because these systems share information, whether it is through the Internet or another information sharing provider, their openness makes them highly susceptible to electronic sabotage.[22] However, centralized information exchange systems are not the only targets. Computer virus warfare (CVW) "poses an interesting problem to manufacturers of advanced combat platforms where the trend is for increased reliance on software to operate many of the key sub-systems; such as sensors, command networks, and even flight controls."[23] Viruses in the form of logic bombs and trojan horses can be installed in software programs. "With the witting or unwitting cooperation of a software manufacturer, a "trap door" can easily be written into almost any commercial software application."[24] Trap doors, whether as software or hardware mechanisms, are often times added as a safety measure by a programmer or manufacturer to bypass a system hang up due to glitches in the program or its hardware. With this ability to use a back door to go around security features in the program, there is a means to fix bugs, no matter what the problem may be.

The arsenal to do battle in Cyberspace will also include radio frequency (RF) weapons. By the synchronous pulsing of electromagnetic energy at a specific frequency, digital signals (logic ones and zeroes) can be emulated. Utilizing this method would allow for the manipulation of data as well as the remote insertion of viruses.[25] Data manipulation is one area which will provide an attacker with a wide array of possibilities to exploit.

The age-old practice of utilizing spies will continue in Cyberspace due to the potential advantages which can be achieved. All facets of Cyberspace are vulnerable; including system network managers, software, and hardware production personnel bringing a new dimension to war. Compromised software and bobby-trapped computer chips could be inserted during the manufacturing process of weapons and $C^2$ systems. The compromised chips may not be identified until in a hostile situation;[26] in the heat of battle it will be too late to start swapping out computer chips, if the problem becomes apparent at all.

## Employment of Weapons in Cyberspace

The contestants on the common ground of Cyberspace will employ a wide variety of methods. However, the basic goals of Cyberspace weapons will be the denial, destruction, and exploitation of information or any combination thereof.[27] Just as there is a wide spectrum of weapons which can be used, there are also many means to use them.

Viruses and logic weapons may be injected directly into a system or network. Known as a "direct launch," such a method may not discriminate and could lead to possible fratricide or collateral damage, requiring the protection of ones own COG.[28]

"Forward basing," like "direct launch" describes another method of introducing weapons into a system or network. The difference is that these weapons lie dormant, waiting for an event to take place or to be triggered or activated when required.[29] Such weapons could allow for operational sequencing by being part of a larger arrangement of events to attack an enemy's COG. By employing a barrage of these weapons into various targeted systems, operational synchronization could be achieved as the weapons worked in concert producing a synergistic effect. Operational phasing could also be achieved as one group of weapons achieved their objective which would then trigger another group of weapons into action.

Although DoD and Joint Publication 1-02 defines directed energy weapons as systems capable of destroying or damaging enemy equipment,[30] the use of directed energy, such as coherent RF signals, would provide for a non destructive method for "remote insertion" of "directed-energy viruses" into a system or network via an unprotected port such as a modem or power supply.[31]

"Hacking" is a well publicized method which utilizes the various cyber weapons to gain access, deny, exploit, or destroy a system. As early as 1994, unclassified documented cases of compromise to Department of Defense (DoD) computers were made known by the Government Accounting Office (GAO). The computer systems of the Air Development Center, the Air Forces's laboratory in Rome N.Y., where the DoD conducts some its research on weapons systems was accessed by two computer hackers. During the several days when access was gained, the intruders were able to gain complete access on all information including wartime methods used by Air Force commanders to relay secret intelligence and targeting information.[32] During this time, with complete access, the hackers could have installed a virus which could have done severe damage.[33] This same incident also revealed the vulnerability that the Internet has in networking with other computers and which is how many of the DoD's computers disseminate information including the possibility of computer viruses. During the same hacking incident, illegal access was made into "military, government, commercial, and academic systems worldwide" of which Wright-Patterson Air Force Base and Goddard Space Flight Center were just two of the systems that were compromised.[34] The occurrence of compromise of such systems, especially in DoD, is growing at a rapid rate. The GAO estimates that 250,000 hacker attacks occurred on DoD computers in 1995 and that figure will double every year.[35]

## The Critical Factors

Operational art teaches that the identification of both enemy and friendly critical factors (critical strengths and critical weaknesses) is key to success in war. For by identifying the enemy's critical strengths, their destruction or neutralization will weaken the COG. Identifying the enemy's critical weaknesses can allow for further analysis in determining critical vulnerabilities if those weaknesses are associated with the COG [36] This analysis will also aid in determining where the sector of main effort will be focused and the decisive points to be achieved.

Cyberspace itself is at the same time a critical strength and a weakness. As a strength, it enhances all facets of the operational scheme. Various methods (cyber weapons employment) of defeating an opponent can be utilized through direct or indirect attacks on both tangible and intangible objectives via Cyberspace. Points of main attack are accessible through the application of cyber weapons. They can be used to carry out operational deception or for operational fires. The use of logic weapons allows for operational sequencing, synchronization, pause, and phasing.

As a weakness, the global connectivity of Cyberspace allows for reciprocative exploitation of unprotected U.S. critical factors. By providing an adversary the ability to reciprocate attacks, unprotected critical strengths and weaknesses operating through the utility of Cyberspace can become critical vulnerabilities. Cyberspace could be considered a critical vulnerability since it affords a globally accessible and unprotected medium for systems to network in. Unprotected critical strengths or weaknesses, that utilize an unprotected Cyberspace, can become critical vulnerabilities. " Sometimes critical strengths, such as C4I or excellent logistical support and sustainment, can become critical vulnerabilities. This is true if various elements of these capabilities are insufficiently protected and thereby potentially open to our attack." [37]

With the advantages that computers provide in determining supply requirements, tracking deliveries, and allocating requirements, computerized logistical systems in the U.S. are lucrative targets. Disrupting systems or networks which exchange such information could hamper successful employment of logistical support. During Desert Storm, about 98% of the logistics' information was processed through unclassified, commercial communications of which the least controllable was the Internet.[38] Although there has been no "creditable method" to cause a complete shut down of the Internet, the possibility looms. Until such time that it happens, the Internet remains as a viable and effective "auxiliary" to a military network that could be easily compromised in war or peace.[39] For the military logistician, the ability to enhance logistics information exchange will be accomplished through the Global Transportation Network (GTN). But even this new system, which fuses transportation information from numerous sources including commercial carriers and shippers, may be susceptible to attack since it will utilize public switched telephone networks in part of the information exchange scheme.[40] Due to the highly developed infrastructure within the U.S. , this critical strength can be highly vulnerable to attack if not adequately protected.

Modern, computerized industrial bases open up a whole new realm of potential critical strengths and weaknesses to attack via Cyberspace. Production lines, R&D efforts, and employment driven by computers are all vulnerable.[41] By inducing errors in the R&D efforts in a system's development, a country could be denied the use of the new capability. Confidence in developing such technology might even wane thereby keeping it from exploring other innovative methods. Such infrastructures are vulnerable to "forward basing" of agents as well as "remote strikes" by hackers.

U.S. $C^2$ infrastructures including those which support transportation such as rail systems and civil aviation are critical strengths. The complex network which synchronizes their movement is vulnerable to compromise. Undermining their safety and reliability would ultimately undermine the confidence of the public which depends on these systems for transportation. $C^2$ vulnerabilities also include a nation's "civilian and strategic leadership, the decision process, societal support structures such as the police, and other governmental entities like the Bureau of Land Management and the strategic oil reserves. Attacking these targets can sow discord in an opponent's society, thereby fracturing the decision-making process or any consensus; deny an opponent the ability to marshal needed resources to rebuff an attack; or divert attention from other activities."[42] With the deleterious effect on the national will, this critical strength also becomes a COG. With the development of GCCS, the military will have a secure (encrypted) method to exchange information up to the highest levels of decision makers (NCA).[43] Consequently, it will be the unprotected $C^2$ system in the civilian sector which could gravitate to become a critical vulnerability and a possible COG.

Utilities such as electrical power plants and phone service providers in the U.S. which rely on networked computers to manage and distribute the flow of power and relay phone calls are critical strengths. However, with an interface into Cyberspace, power plants which feed into a power grid are susceptible to the targeting of their control systems which allow for the distribution of power. Creating power sinks by draining power out of the grid could lead to massive brown-and blackouts.[44] A massive loss of phone service could induce chaos, especially if it were coupled with a severe power loss. Consequently, such systems if operating unprotected can become critical vulnerabilities.

The critical strength of the U.S. economic sector provides myriad possibilities for attack via Cyberspace. Computers are infused into the control mechanisms of debt, tariffs, price controls, and exchange rates.[45] Banks and other financial institutions rely on automated methods to transfer money. ATMs are a mainstay in the U.S. Rand Corporation's wargame, "The Day After...in Cyberspace," which was played by senior U.S. officials revealed key items to exploit in bringing a nation to the bargaining table during future conflicts: degradation of computer controlled assets such as satellite surveillance, communications, commercial aviation, banking, and information exchange systems in business were pivotal in producing victory in the age of information war.[46] Attacks on these "selected nodes of American social and economic fabric..." would produce strategic results.[47] Confidence would wane in the economy as the data bases for financial markets, stock exchanges and banking systems were manipulated to produce deleterious interest rates, substandard profits, and losses to savings. Targets could be prepped months or years in advance and subtly attacked. The strategic repercussions alone provides the impetus for any knowledgeable adversary: terrorist, guerrilla, or rogue nation, to employ a focused effort in compromising these systems.[48] Unprotected, this critical strength could become a critical vulnerability and a possible COG.

The critical strength of U.S. public transportation, which has come to depend on computers to make travel efficient, is also susceptible to exploitation. The psychological effect of removing the efficiency, dependability, and potential of such a system could induce "cascading chaos"; hampering efficient transportation means a society may be without the basics for sustenance, or weapons and fuel to carry on a war could be diverted or lost in a massive and complex transportation infrastructure.[49]

Military training becomes an exploitable intangible critical strength if a nation fights as it trains. By manipulating statistics and data bases or by incorporating tainted information into a resulting training scheme, a compromised system of training could be generated. One method of subversion would be for an adversary to "leak" an altered training manual to the nation which it had planned to attack.[50] Lack of training in computer systems security is a critical weakness which the Defense Information Systems Agency (DISA) has been grappling with since 1992 when it developed "Red Teams" to attack friendly computer networks in order to assess vulnerability. Since that time, 38,000 attacks were initiated with 65% having breached the computers with the disheartening fact that only four percent of attacks were recognized by system administrators.[51]

## Critical Vulnerabilities:

With the proliferation of information age hardware and software and the ever-shrinking technology life cycle, DoD has shifted from "being the driving force in information technology to being a specialty user...."[52] Austere budgets have forced the DoD to forego development of specialty high technology systems and rely on commercial-off-the-shelf (COTS) technology to allow for timely acquisition and in order to "field cost-effective systems."[53] In addition, there are "aging systems" that need replacement to ensure that continued readiness is maintained.[54]

COTS technology inherits vulnerabilities some of which computer viruses can exploit. Military systems will now be based on systems architectures and components which are available to any potential adversary to systematically investigate. They can produce tailored computer viruses to target the associated hardware and supporting software. Captured military equipment, especially highly developed and non-COTS technology, is also susceptible to hardware and software compromise. A determined adversary can reverse engineer a system and develop computer viruses to be used immediately or in the future. The nature of the virus could be to cause complete failure of a system or to inject tainted information. The latter will produce uncertainty in the quality of information and tax decision makers at all levels of command and control. Such a vulnerability will require "unique keys that identify and authorize users on particular systems, devices that report current locations on key hardware items via satellite, authentication procedures, and security codes" to combat the exploitation of such systems.[55]

In the defense sector, where computer software has provided the enhanced capabilities for equipment and systems, the vulnerabilities are just as ominous.[56] Software has basically "touched" every piece of military hardware, and since "no software is completely testable because of the large number of possible execution paths...",[57] the threat of compromised systems could certainly be diverse and substantial. But what characterizes such risk is the fact that tampered software can be an insidious threat. In affected systems, the normal external operation of that system may in fact belie an embedded weakness only to be revealed when it is too late to do anything about it.

### Protection in Cyberspace

The common link that is shared by the computer dependent critical factors is the information infrastructure and associated connectivity which make up Cyberspace. One method in protecting the information exchange has been through encryption. However, due to incompatibility and standardization, establishing an encryption system capable of communicating on a network with foreign allies and especially within a diverse civilian sector is a problem.[58] For the U.S. military, systems such as GCCS will provide the protection and security required to exchange sensitive information. But this does not solve the problem for the previously sanctuaried critical factors. Although encryption can make it much more difficult for an adversary to compromise a system, risks still remain. As long as there is an electronic link (computer interconnectivity) or a medium to utilize directed energy weapons, critical strengths and weaknesses are susceptible to destruction, denial, or compromise. In the civilian sector, where encryption methods are utilized in but a few of the economic sectors, operational security will have to rely on awareness. The key to improved security in the short term is increased awareness of the potential damage network breaches can cause.[59]

## Conclusion

In 1996, DoD had over "2.1 million computers, 200 command centers, 16 central computing "MegaCenters," 10,000 local networks and 100 long-distance networks,...."[60] Coupled with the trend for increased utilization of COTS and software enhanced systems, the increased push to employ the utility of Cyberspace brings with it an exponential increase in vulnerabilities to economic, military, social, and political critical factors. The lever arm of technology and its offspring; cyber weapons, will expose the sanctuaried critical factors. "The implications of warfare in the information arena are enormous. First, national homelands are not sanctuaries. They can be attacked directly, and potentially anonymously, by foreign powers, criminal organizations, or non-national actors such as ethnic groups, renegade corporations, or zealots of almost any persuasion. Traditional military weapons cannot be interposed between the information warfare threat and society."[61]

Encryption methods and operational security training will afford some protection, but incompatibility between the vast types of networked systems and the continually shrinking technology life cycle in both sectors will remain a problem as distinctions between military and non-military systems become hard to differentiate. The National Security Agency estimates that there are more than 120 nations that have established "information warfare cadres" which are designed to take advantage of an adversary's weaknesses in operational security.[62] The return on the investment in a simple computer system equipped with a modem provides the potential to effect multi-billion dollar damage on a high tech military.

U.S. planners, especially at the strategic and operational levels, must appreciate the complexity in planning for defenses and protection of U.S. critical factors; for with the new opportunities in Cyberspace come vulnerabilities. Strategic geography and military force has been made transparent by the global connectivity afforded by Cyberspace.

# Notes

[1] David S. Alberts, *The Unintended Consequences of Information Age Technologies* (Washington, D.C.: National Defense Univ., 1996), 27.

[2] Steve Lambert and Walt Howe, *Internet Basics* (New York: Random House 1993), 459.

[3] Office of the Joint Chiefs of Staff, *Joint Command and Control, Communications, and Computers Systems Descriptions Volume I* (Washington D.C.: 1994), 84.

[4] Mark Mateski, "Beyond Metaphors: Information Warfare and Systems Thinking," *Jane's US Information Warfare E-Letter*, 27 January 1997, 1.

[5] *The Littoral and Information Warfare Conference*, unpublished conference presentation notes, U.S. Naval War College, Newport, R.I.: 3 March 1995, III-6.

[6] Stephen M. Hardy, "Should We Fear the Byte Bomb?," *Journal of Electronic Defense*, January 1996, 45.

[7] Ibid.

[8] Stephen M. Hardy, "The New Guerrilla Warfare." *Journal of Electronic Defense*, September 1996, 50.

[9] Hardy, "Should We Fear the Byte Bomb?," 45.

[10] Ibid., 45.

[11] Mark Thompson, "If War Comes Home," *Time*, 21 August 1995, 46.

[12] Mark Bently and Paul Evancoe, "CVW - Computer Virus as a Weapon," *Military Technology*, May 1994, 38.

[13] Ibid.

[14] Ibid., 39.

[15] Center for Naval Analyses, *Offensive Information Warfare--A Concept Exploration.* (CIM 361. Alexandria: VA. 1994.) 17.

[16] Bently and Evancoe, 39.

[17] Ibid.

[18] Center for Naval Analyses, 6.

[19] Ibid.

[20] Bently and Evancoe, 39.

[21] Hardy, "Should We Fear the Byte Bomb?," 45.

[22] Michael Howard and John F. Guilmartin, Jr. *Two Historians in Technology and War* (Strategic Studies Institute, U.S. Army War College, Carlisle Barracks, PA. July 1994.) 33.

[23] Bently and Evancoe, 40.

[24] Center for Naval Analyses, 6.

[25] Ibid.

[26] Douglas Waller, "Onward Cyber Soldiers," *Time*, 21 August 1995, 41.

[27] Center for Naval Analyses, 10.

[28] Ibid.

[29] Ibid.

[30] Office of the Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms*, Joint Publication 1-02 (Washington, D.C.: 1984) 117.

[31] Center for Naval Analyses, 10.

[32] Philip Shenon, "Report Warns of Security Threats Posed by Computer Hackers," *The New York Times*, 23 May 1996, A22:1.

[33] Howard and Guilmartin, 33.

[34] Shenon, A22:1-2.

[35] John J. Fialka, "Pentagon Hacker Attacks Increase And Some Pose Threat, GAO Says," *The Wall Street Journal*, 23 May 1996, B3:1.

[36] Milan N. Vego, "Elements of Operational Warfare," NWC 4096, unpublished paper, U.S. Naval War College, Newport, R.I.: August 1996, 3.

[37] Ibid.

[38] Hardy, "The New Guerrilla Warfare," 48.

[39] Ibid., 50.

[40] *Joint Command and Control, Communications, and Computers Systems Descriptions Volume I*, 89.

[41] Center for Naval Analyses, 12.
[42] Ibid.
[43] *Joint Command and Control, Communications, and Computers Systems Descriptions Volume I*, 84.
[44] Center for Naval Analyses, 13.
[45] Ibid., 12.
[46] Thompson, 45-46.
[47] Howard and Guilmartin, 34.
[48] Richard O. Hundley and Robert H. Andersen, *Security In Cyberspace: An Emerging Challenge For Society,* RAND, P-7893, 1994, 6.
[49] Center for Naval Analyses, 14.
[50] Ibid.
[51] Hardy, "The New Guerrilla Warfare," 48.
[52] Alberts, 27.
[53] Ibid.
[54] "Commercial Information Systems Proliferate in Military Operations," *Signal*, January 1997, 63.
[55] Alberts, 41.
[56] Peter Emmett, "Information Mania-A New Manifestation of Gulf War Syndrome?" *RUSI Journal*, February 1996, 23.
[57] Ibid.
[58] Hardy, "The New Guerrilla Warfare," 52.
[59] Hundley and Andersen, 49.
[60] Hardy, "The New Guerrilla Warfare," 48.
[61] Alberts, 27.
[62] Hardy, "The New Guerrilla Warfare," 50.

# Bibliography

Alberts, David S. *The Unintended Consequences of Information Age Technologies.* Washington, D.C.: National Defense Univ., 1996.

Bently, Mark and Paul Evancoe. "CVW - Computer Virus as a Weapon." *Military Technology*, May 1994, 38-40.

Center for Naval Analyses. *Offensive Information Warfare--A Concept Exploration.* CIM 361. Alexandria, VA: 1994.

"Commercial Information Systems Proliferate in Military Operations." *Signal*, January 1997, 63-65.

DOD 5200.28-STD, *Department of Defense Trusted Computer System Evaluation Criteria*, December 1985.

Emmett, Peter. "Information Mania-A New Manifestation of Gulf War Syndrome?" *RUSI Journal*, February 1996, 19-26.

Fialka, John J. "Pentagon Hacker Attacks Increase And Some Pose Threat, GAO Says." *The Wall Street Journal*, 23 May 1996, p. B3:1-2.

Hardy, Stephen M. "Should We Fear the Byte Bomb?." *Journal of Electronic Defense*, January 1996, 42-47.

________. "The New Guerrilla Warfare." *Journal of Electronic Defense*, September 1996, 46-62.

Howard, Michael and John F. Guilmartin, Jr. *Two Historians in Technology and War.* Strategic Studies Institute, U.S. Army War College, Carlisle Barracks, PA. July 1994.

Hundley, Richard O. and Robert H. Andersen. *Security In Cyberspace: An Emerging Challenge For Society.* RAND, P-7893, 1994.

Lambert, Steve and Walt Howe. *Internet Basics*. New York: Random House, 1993.

Mateski, Mark. "Beyond Metaphors: Information Warfare and Systems Thinking," *Jane's US Information Warfare E-Letter*, 27 January 1997.

Office of the Joint Chiefs of Staff, *Joint Command and Control, Communications, and Computers Systems Descriptions Volume I* (Washington D.C.: 1994)

Office of the Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms*, Joint Publication 1-02 (Washington, D.C.: 1984)

Shenon, Philip. "Report Warns of Security Threats Posed by Computer Hackers." *The New York Times*, 23 May 1996, p. A22:1-6.

*The Littoral and Information Warfare Conference*, unpublished conference presentation notes, U.S. Naval War College, Newport, R.I.: 3 March 1995.

Thompson, Mark. "If War Comes Home." *Time*, 21 August 1995, 44-46.

Waller, Douglas. "Onward Cyber Soldiers." *Time*, 21 August 1995, 38-44.

## Additional Reading

Barnaby, Frank and Marlies ter Borg. ed.,*Emerging Technology and Military Doctrine*. New York: St. Martins Press Inc, 1986.

Blackwell, James and Anthony H. Cordesman, *Strategy and Technology*. Strategic Studies Institute, U.S. Army War College, Carlisle Barracks, PA. April 1992.

Emmett, Peter. "Software Warfare: The Militarization of Logic," *Joint Forces Quarterly*, Summer 1994; 84-90.

Jeremiah, Adm, David E. "How Rapid Technological Change Will Change Warfare." *Asia-Pacific Defence Reporter*, October-November 1993, 26-27.

Libicki, Martin C. *What is Information Warfare?* Washington, D.C.: National Defense Univ., 1995.

"Panel to Oversee Protecting Systems From Hackers." *The Wall Street Journal*, 17 July 1996, p. B8:1.

Shukman, David. *Tomorrow's War The Threat of High-Technology Weapons*, New York: Harcourt Brace, 1996.

Weiner, Tim. "Head of C.I.A. Plans Center To Protect Federal Computers." *The New York Times*, 26 June 1996, p. B7:5.